Virussen

Onkruid vergaat niet

Het ziet er naar uit dat we binnenkort ook een Stevaert nodig hebben om aan onze vírtuele verkeersveiligheid te timmeren… Het internet lijkt namelijk wel een broeinest geworden van spammers, hackers en niet in het minst ook… virussen! Wie zijn ze, wat doen ze en – vooral – hoe kan je je ertegen beschermen?

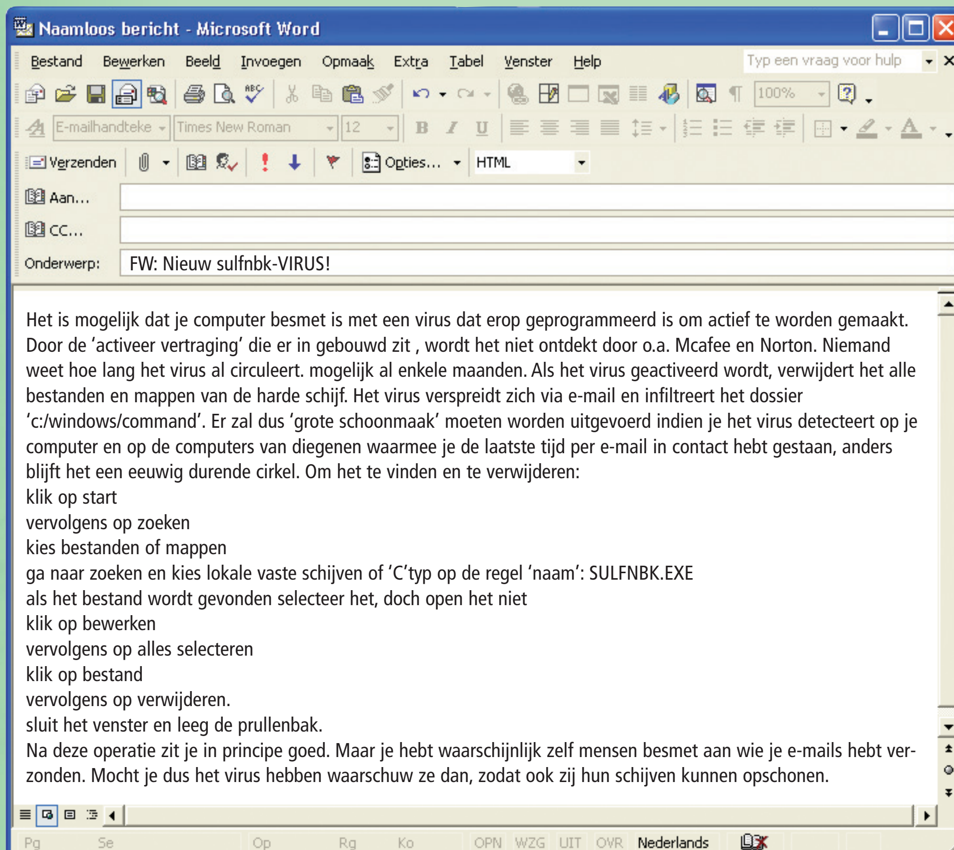




Jean koos dit dossier.

Ga, en vermenigvuldig u!

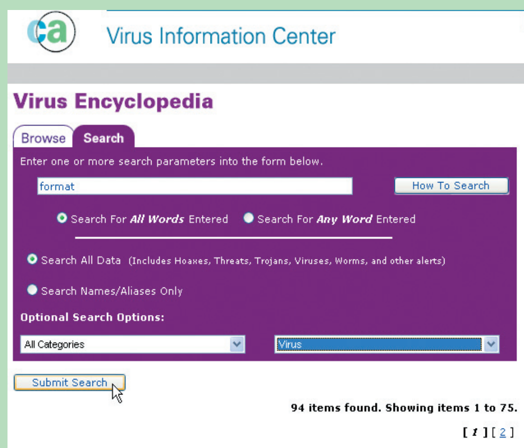
Ontdaan van alle geheimzinnigheid schiet er van een typisch computervirus weinig meer over dan een klein programmaatje dat er vooral op gericht is zichzelf zo snel mogelijk te vermenigvuldigen. In principe heeft zo'n virus daarbij de hulp nodig van een ander programma(bestand), bij voorkeur eentje dat de gebruiker geregeld opstart. De viruscode hecht zich dan aan dat legitieme programma en zodra de gebruiker dat uitvoert, wordt meteen ook het virus mee opgestart en in het geheugen geladen. Van daaruit ligt het dan op vinkenslag en probeert het nog meer programmabestanden te infecteren. Als je het kaderstukje doorneemt, heb je echter al snel door dat virusmakers erg inventief kunnen zijn als het eropaan komt geschikte slachtoffers te vinden voor hun virale infecties.
Sommige virussen, de zogenaamde wormen, hebben strikt genomen zelfs geen ander bestand nodig om zichzelf te kunnen verspreiden. Die maken gewoonlijk dankbaar gebruik van e-mail om zich van de ene naar de andere computer te verplaatsen. Heel vaak werken die volgens het principe van een kettingbrief: zo'n mailworm komt toe bij een gebruiker waar hij ongemerkt zijn adresboek uitleest en zichzelf vervolgens doormailt naar al die mailboxen. Daar gebeurt natuurlijk weer hetzelfde en op die manier begrijp je dat zo'n worm zich exponentieel kan vermenigvuldigen en uiteindelijk zelfs hele netwerken en delen van het internet lam kan leggen!
Hoaxes (letterlijk: flauwe grappen) zijn ook een soort worm. Dat zijn e-mailberichtjes die je om de haverklap toegestuurd krijgt en waarin je op indringende wijze gewaarschuwd wordt voor één of ander nieuw supervirus. Vast onderdeel is de vraag om dit bericht zo snel mogelijk naar iedereen uit je adresboek door te sturen. Zo'n bericht is bijna altijd vals, maar het krijgt wel zelf de allures van een worm als iedere ontvanger inderdaad op die vraag zou ingaan! Niet doen dus! Een heel populair exemplaar is bijvoorbeeld nog steeds de SULFNBK-hoax die je waarschuwt voor een virus dat zich mogelijk al op je pc heeft genesteld, meer bepaald in de vorm van het bestand sulfnbk.exe. Dat is echter een onschuldig systeembestand van bepaalde Windows-versies en wis je dus maar beter niet! Op [www.vmyths.com] vind je een heel uitgebreid overzicht van bekende hoaxes. In Clickx 34 vind je meer info over hoaxes.



Een hoax: virtuele kletskoek!

Aanvalleeuuuh!

Virusmakers krijgen hun kick dan wel vooral van een snelle verspreiding van hun creaturen, blijkbaar is er in zo'n zieke geest nog ruimte voor wat extra geinigheid... Niet zelden zit er in zo'n virus ook een incubatieperiode ingebouwd: tijdens deze sluimertijd doet het virus niks anders dan zich verspreiden, maar zodra die periode voorbij is, schiet er een destructievere module in dat virus wakker. Wat het virus dan precies met je computer uitspookt, hangt vooral af van hoe perfide zijn maker wel was: bepaalde bestanden worden onherroepelijk gewist, gegevens in je spreadsheets worden aangepast, je harde schijf wordt zomaar even geformatteerd, enz... Zonder enige vorm van bescherming ben je dus overgeleverd aan de willekeur van de virusmaker!
Een virusachtig fenomeen waarin ook zo'n 'verborgen agenda' zit ingebouwd, is het Trojaanse paard, dat zich vaak verstopt achter een of ander nuttig programma dat je bijvoorbeeld hebt gedownload van het net of als e-mailbijlage hebt ontvangen. Op het eerste zicht schuilt er geen kwaad in het programma en kan je het zelfs nuttig inzetten. Maar zonder dat je het weet, doet het ook nog iets anders. Heel typisch zet het bijvoorbeeld bepaalde



80.000 exemplaren... een flinke encyclopedie!

poorten van je computer open zodat de maker van het paard via het internet contact krijgt met je computer en die voor allerlei doeleinden kan misbruiken. Zo kan hij bijvoorbeeld delicate gegevens – is je kredietkaartnummer delicaat genoeg? – aan je harde schijf ontfutselen, of op een bepaald moment alle pc's waarop zijn Trojaans paard is geïnstalleerd, de opdracht geven één of andere (bekende) website met informatieverzoeken te bombarderen. Die webserver kan het verkeer niet langer slikken en geeft er dan maar de brui aan. Zo'n georchestreerde aanval – waaraan jij dus ongewild hebt meegewerkt! – noemen we een DDoS (Distributed Denial of Service Attack). Je merkt het: er is een heel oerwoud vol venijnige beestjes – en intussen zijn er al zo'n 80.000 geteld, varianten inclusief. Heb je daar een gezonde interesse voor, dan kan je op het net verschillende virusencyclopedieën raadplegen. Eén van de bekendste is het Virus Information Center [**www3.ca.com/virusinfo/Encyclopedia.asp?MODE=BROWSE**], waarin je kan bladeren of opzoekingen verrichten in een uitgebreid alfabetisch overzicht van hoaxes, virussen, wormen en Trojans. Ook Symantec laat zich niet onbetuigd, en komt met een eigen viruslijst op [**http://securityresponse.symantec.com/avcenter/vinfodb.html**].

Steeds venijniger...

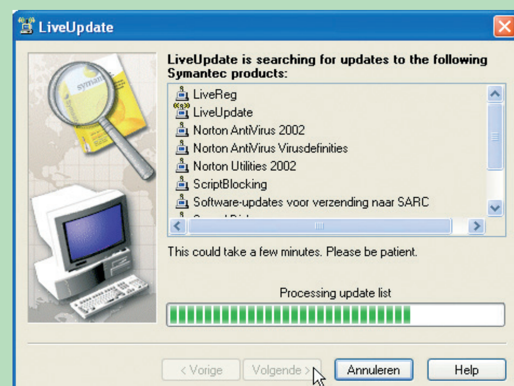
Er komen niet alleen steeds méér virussen, ze worden ook intelligenter en complexer, en zijn daardoor meteen moeilijker te detecteren. De eerste generaties virussen staken nogal simpel in elkaar: zo bevatte elk virus een vast bytepatroon – een soort DNA-string zeg maar – dat in elke infectie van dat virus terugkeerde. Voor een antiviruspakket was het dan een koud kunstje om zo'n besmetting te detecteren: het hoefde dat bytepatroon of virushandtekening dan maar in zijn databanken te hebben om de dader te ontmaskeren.
Wil je overigens zelf zo'n onschuldig (!) virus in elkaar knutselen, dan hoef je alleen maar de volgende tekst zonder spaties in je Kladblok in te tikken:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EI-
CAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

Dit bestandje sla je dan bijvoorbeeld op onder de naam 'testvirus.com'. Hou er wel rekening mee dat je antivirusprogramma alarm slaat zodra je op dit bestand dubbelklikt! De virushandtekening van dit bekende testvirus hoort namelijk in de databank van elke antiviruspakket te zitten.
Virusmakers moesten dus met lede ogen aanzien hoe hun product snel door antivirusprogramma's werd gedetecteerd. Al snel bedachten ze daarom allerlei technieken om hun geesteskind beter te camoufleren: de viruscode werd bijvoorbeeld versleuteld of zag er bij elke infectie telkens netjes anders uit (polymorf), zodat het heel moeilijk werd naar een vast bytepatroon te speuren! Dergelijke stealth-virussen zijn overigens nu meer regel dan uitzondering en ze maken het de antiviruspakketten knap lastig. Maar virussen zijn ook nog op een ander niveau geëvolueerd... Experts hebben het over 'gecombineerde bedreigingen' (Blended Threats). Dat zijn virusachtige ondingen waarbij de scheidingslijn tussen hacks (inbraakpogingen), wormen, virussen en Trojaanse paarden vervaagt. Een typisch voorbeeld hiervan is het bekende Klez-virus. Dat is weliswaar een worm die zich via e-mail verspreidt, maar in de bijlage van het virus zit ook nog zo'n polymorf virus verborgen dat je lokale bestanden kan besmetten. Tegelijk zet de worm ongemerkt een eigen *mailserver* (de vaktaal vind je in het midden van dit nummer) op, speurt hij naarstig naar e-mailadressen op je schijf, en verstuurt hij zichzelf vervolgens door naar al die mailboxen. Een ander voorbeeld is het notoire Nimda-virus dat zich langs twee kanalen tegelijk kon verspreiden: enerzijds via e-mail, anderzijds nestelde het zich op webservers zodat je ook via je browser geïnfecteerd kon worden zodra je een webpagina op zo'n *server* bezocht.
Je begrijpt dus dat antivirusmakers hun handen vol hebben met al die vandaalsoftware! Zo volstaat het speuren naar vast herkenbare virushandtekeningen al lang niet meer en de meeste pakketten maken dan ook gebruik van complementaire methodes zoals heuristische scans. Daarbij wordt elk potentieel virusbestand in een beschermde omgeving uitgevoerd en gaat het antiviruspakket meteen na of er zich in de programmacode geen verdachte instructies bevinden, zoals 'formatteer even die partitie'. Met wat geluk weten antivirusprogramma's op die manier zelfs onbekende virussen te strikken!



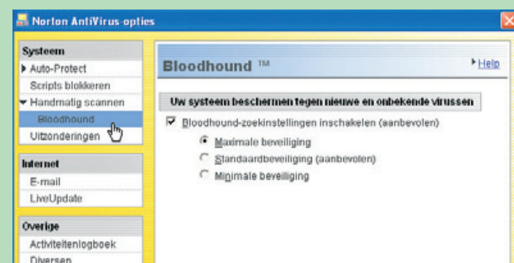
Je eigen virus wordt wel onderschept, maar hoe zit het met de rest?



Niet van gisteren toch, je antiviruspakket?

In het verweer!

Er zijn natuurlijk een flink aantal van die pakketten op de markt, zoals je al kon lezen in onze test van antivirussoftware in Clickx 34. Zo is er de bekende Norton AntiVirus 2003 (gratis proefversie op [**www.symantec.com/nav/nav_9xnt**], McAfee VirusScan 7.0 [**www.mcafee.com/myapps/vs7**], en F-Secure Anti-Virus (gratis proefversie op [**www.f-secure.com/download-purchase/list.shtml**]). Helemaal gratis kan ook nog, tenminste voor persoonlijk gebruik: AVG 6.0 [**www.grisoft.com**] en relatieve nieuwkomer Avast! Antivirus Home Edition 4 [**www.avast.com/avast4**]. Al deze producten scoren behoorlijk in diverse tests, maar heel belangrijk blijft evenwel dat je steeds over de meest recente versies beschikt én dat je de virusdefinities waarvan het pakket zich bedient, up-to-date weet te houden. De meeste pakketten zorgen daar trouwens automatisch zelf voor, tenminste als je over een semi-permanente internetverbinding als kabel of *ADSL* beschikt. Zo goed als alle antiviruspakketten nemen ook volautomatisch in- en uitgaande e-mail voor hun rekening, en zo



De bloedhond van Norton: heuristische speurneus.

Even tussendoor, een gratis on line scanronde.

hoort het ook! De meeste virussen en wormen verspreiden zich immers vooral langs die weg. Ook al is je antivirusprogramma continu op de achtergrond actief (on-access), toch doe je er goed aan je ganse systeem af en toe ook eens grondig uit te borstelen. Een dergelijke antivirusoperatie noemen we wel 'on-demand', en elk goed antiviruspakket laat je op elk moment de opdracht tot zo'n grote kuis geven. Sommige gebruikers geraken echter zo paranoïde dat ze twee antivirusprogramma's tegelijk installeren en die alles in de gaten laten houden. Geen goed idee overigens, want niet zelden zitten twee van dergelijke virusjagers elkaar in de haren, zodat hun werking onbetrouwbaar wordt.
Je doet er dan beter aan je vaste antivirusprogramma desnoods tijdelijk even uit te schakelen en een gratis on line scanronde op je systeem los te laten. Voordeel is dat zo'n on line scan tenminste up-to-date is. Op [**www.ravantivirus.com/scan**] vind je zo'n scanmodule waarmee je je hele pc of selectief bepaalde mappen, bestanden of e-mailberichtjes kan laten scannen. Wil je geïnfecteerde bestanden laten verwijderen, vergeet dan niet een vinkje te plaatsen naast de optie Autoclean! Voor andere on line scans kan je terecht bij Trend Micro [**http://housecall.antivirus.com**] en bij Symantec [**http://security.symantec.com**]. Minpuntje van deze laatste is wel dat je niet selectief op bepaalde onderdelen kan laten scannen.
Ten slotte, hoor je van een of ander virus dat plots de kop heeft opgestoken, dan kan het nooit kwaad eens langs te lopen bij de sites van bekende virusjagers als Symantec of McAfee. Niet zelden plaatsen die op hun webstek snel een remedie tegen één welbepaald virus.

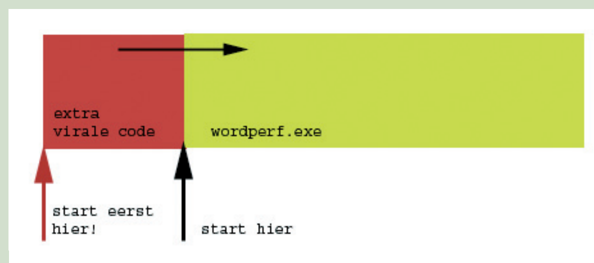
Gezond boerenverstand

Een up-to-date antiviruspakket hoort dus centraal te staan in je verdedigingsstrategie. Dat neemt niet weg dat je ook andere voorzorgsmaatregelen hoort te nemen. Heel wat virussen maken namelijk misbruik van bepaalde veiligheidslekken in besturingssystemen als Windows of in populaire programma's als Outlook (Express) en Internet Explorer. De producenten van die software proberen de meeste veiligheidslekken te dichten door het publiceren van allerlei programmaatjes, *patches* genoemd. Die kan je dan gratis downloaden op hun websites. Werk je met Windows, laat dan zeker niet na geregeld een bezoek te brengen aan [**http://windowsupdate.microsoft.com**]: hier tref je namelijk frequent *updates* en patches aan die de bekendste veiligheidslekken (horen te) dichten. Ben je bang dat één of ander Trojaans paard vanop je pc heimelijk gegevens naar de maker doorsluist, dan kan je ook nog een persoonlijke *firewall* installeren – ook al is die er in de eerste plaats op gericht hackers buiten te houden. Een heel populair voorbeeld is ZoneAlarm, waarvan je een gratis versie kan sponzen op [**www.zonelabs.com**].
Ten slotte, geen enkele antivirusstrategie kan zonder een flinke dosis gezond boerenverstand! Ontvang je bijvoorbeeld een mailtje-met-bijlage van een onbekende, open het dan niet en kieper het bij voorkeur meteen in de vuilnismand. Zelfs met bijlagen van kennissen hoor je nog voorzichtig te zijn... want wie weet heeft Klez op dat moment al lelijk huis gehouden op hun computersysteem! Een gewaarschuwd man...

— Toon Van Daele —

ONWILLIGE GASTHEREN...

Een klassiek virus heeft normaal een stukje uitvoerbare programmacode nodig waaraan het zich kan hechten, net als een parasiet. De oudste virussen nestelden zich nogal eens op een speciale plaats van een harde schijf of diskette. Dat is de zogenaamde bootsector, en de instructies die daarop terechtkomen worden bij (een poging tot) het opstarten van die schijf automatisch uitgevoerd. Andere virussen richten hun pijlen vooral op uitvoerbare bestanden als de gekende .com en *.exe*-bestanden. Voerde je zo'n bestand uit, dan greep meteen ook het parasitaire virus zijn kans. Van daar was het eigenlijk maar een kleine sprong naar de zogenaamde macro-virussen. Die infecteren niet zozeer een uitvoerbaar bestand, dan wel een gegevensbestand van een Office-programma als Excel of Word. Zodra zo'n besmet bestand in de Office-applicatie wordt ingeladen, worden meteen ook de instructies uitgevoerd die het virus in dat bestand had achtergelaten.



Een parasitair virus bijt zich graag in exe-bestanden vast.